829

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/597,982	06/19/2000	Olli Immonen	367.38672X00	5877

20457 7590 01/15/2004

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-9889

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	6

DATE MAILED: 01/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PRG

Office Action Summary	Application No.	Applicant(s)	
	09/597,982	IMMONEN, OLLI	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on 6/19/2000.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-39 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-39 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-39 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-39 are rejected under 35USC 102(e) as being anticipated by Puhl et al.

In reference to claim 1:

Puhl et. al discloses a tamper evident wireless application protocol identity module (WIM) (Column 12, lines 3-10) including stored thereon a public-private key pair and a manufacturer certificate (Column 5, lines 58-61), wherein the certificate contains a set of fields holding data relating to said key pair, the certificate being signed using a further private key, where the Public Key certificate is the certificate being signed using a further private key (Column 3, line 58-Column 4, line 9).

In reference to claim 2:

Puhl et. al discloses a module wherein the public key is held within a field of said certificate. (Column 3, lines 58-59)

In reference to claim 3:

Puhl et. al discloses a module further including a certification authority certificate. (Column 5, lines 58-61)

In reference to claim 4:

Puhl et. al discloses a module wherein the at least one certificate is stored externally of said module at a remote location which is derivable from an address stored on said module, where the CA server stores both a license certificate and a CA public key certificate, both of which are at an external location, and also derivable from the identity of the certification authority stored on the module. (Column 4, line 54 – Column 5, line 16) Addresses may also be specifically stored in the certificate, also stored within the module. (Column 16, lines 1-13)

In reference to claim 5:

Puhl et. al discloses a module wherein the further private key is the manufacturer's private key, (Column 3, line 58- Column 4, line 9) and, where the manufacturer's private key comes from the CA (Column 4, lines 24-35).

In reference to claim 6:

Puhl et. al discloses a module wherein the further private key is an initial management key, the module further having stored thereon an initial management certificate signed using the manufacturer's private key, where the initial management key is the private key created by the certification authority, and the initial management certificate is the certificate originally created

by the certification authority to be placed on the module. (Column 11, lines 48-57) & (Column 3, line 58 – Column 4, line 9)

In reference to claim 7:

Puhl et. al discloses a method of manufacturing a tamper-evident wireless application protocol identity module(WIM) (Column 12, lines 3-10) comprising the step of:

Storing a public-private key pair on said module together with a manufacturer certificate signed using a further private key. (Column 5, lines 58-61), & (Column 3, line 58- Column 4, line 9) & (Column 17, lines 24-32)

In reference to claim 8:

Puhl et. al discloses a method wherein the key pair is created externally of said module, where the keys are generated and loaded into the module. (Column 17, lines 20-56) & (Column 4, lines 54-61)

In reference to claim 9

Puhl et. al discloses a method wherein the key pair is created internally of said module, where the keys are generated by the module itself (Column 4, lines 54-61), in the creation of the certificate, and the certificate is known to contain the key pairs. (Column 12, lines 18-20) & (Column 17, line 65 – Column 18, line 5)

In reference to claim 10:

Puhl et. al discloses a method, wherein the manufacturer certificate is created externally of the module, where the certificate may be created by the Certificate Authority.

(Column 4, lines 54-61)

In reference to claim 11:

Puhl et. al discloses a method wherein the module is accessed to obtain the public key to facilitate the external creation of the certificate (Column 3 lines 11-14) & (Column 4, lines 54-64) The phone's public key certificate is accessed by the CA to obtain the public key. The CA signs this to create the CA's public key certificate for the phone/ WIM module, binding the phone's public key to its identity. Furthermore, (Column 10, lines 12-16) show that this verification is the process in which an entity becomes "enrolled" into the domain, or the PKI network.

In reference to claim 12:

Puhl et. al discloses a method wherein the further private key is the manufacturer's private key, where the manufacturer's private key is the private key of the certificate authority (Column 4, line 65 – Column 4, line 9), and it is understood from Puhl et al. that the certification authority is the manufacturer. (Column 4 lines 30-35)

In reference to claim 13:

Puhl et. al discloses a method further comprising the steps of:

- Storing an externally created initial management key pair and an initial management certificate signed using the manufacturer's private key on said module, where the initial management key pair are the public and private keys of the module and the initial management certificate is the public key certificate of the module (Column 3, line 58 – Column 4, line 9), the manufacturer's private key used to sign is the private key of the CA, which is understood to be the manufacturer (Column 4, lines 30-35). It is also understood that this Public Key Certificate may be created internally or externally as specified in (Column 4, lines 54-61).
- Storing an internally created manufacturer certificate on said module wherein the further private key is the initial management private key, where the manufacturer certificate is created by an internal process, the public key certificate created by the CA and the private key is the private key internal to the module. (Column 17, line 65 – Column 18, line 5)

In reference to claim 14:

Puhl et. al discloses a method of validating a tamper-evident wireless application protocol identity module(WIM) on which is stored at least one public-private key pair together with a manufacturer certificate signed using a further private key, the method comprising the steps of:

- Querying a public directory to obtain a public key certificate with which to verify the signature generated by the further private key, where the public directory is the directory of the domain (Column 15, lines 23-34). (Column 19, lines 4-11) further discloses the use of this hierarchy in a transaction.

In reference to claim 15:

Puhl et. al discloses a method of validating the identity of a communication terminal for conducting transactions on the network comprising the steps of:

- Establishing the identity of a user of the terminal connected to the network, where the terminal is a entity which wants to connect to the domain, and where identity is established through the private key and public key certificates. (Column 9, lines 41-45)
- Interrogating the terminal to obtain a public key of the public-private key pair stored on the terminal, where the terminal is asked for it's public key as part of the process to enroll it on the domain or network. (Column 10, lines 8-16)
- Conforming the authenticity of a certificate signed by the module manufacturer supporting the public key. (Column 3, line 58 – Column 4, line 9)
- Subsequently issuing a further certificate for the public key which certificate is available to support transactions with the terminal over the network, where the CA public key certificate is directly made available to support transactions with the terminal over the network, and the license certificates, the product certificates are indirectly made available to support transactions with the terminal over the network. (Column 4, line 54 - Column 5, line 61)

In reference to claim 16:

Puhl et. al discloses a method wherein the network service provider carries out the authentication of the manufacturer certificate. (Column 11, lines 48-56)

In reference to claim 17:

Puhl et. al discloses a communications device having stored thereon

- a plurality of certificates supporting security operations including authentication and non-repudiation, where the plurality of certificates include the license certificate, the product certificate, the Public key certificate and the CA public key certificate. (Column 3, line 58 - Column 5, line 61)
- and further including a manufacturer certificate stored on a tamper evident module (Column 12, lines 52-57)
- wherein the manufacturer certificate contains a set of fields holding data relating to a public-private key pair for application layer security, at least the private key being stored on said module, the manufacturer certificate being signed using a further private key, where the manufacturer certificate, the CA certificate is signed by the private key of the CA. (Column 3, line 58 - Column 4, line 9)

In reference to claim 18:

Puhl et. al discloses a device wherein at least one certificate supporting security operations is stored externally of said device at a remote location which is derivable from an address stored on said device. (Column 16, lines 1-20)

In reference to claim 19:

Puhl et. al discloses a method of satisfying an identity module issuer of the provenance of an identity module for use in transactions on a network comprising the steps of:

- Approving, by the issuer, a manufacturing process of the module manufacturer, where the issuer is the certification authority, and approving is performed through the signing of the certificate. It is known in the art that a certification authority in digitally signing a certificate acknowledges a certain level of trust has been fulfilled. (Column 2, lines 56-63) & (Column 4, lines 54-61)
- Storing, by the manufacturer, a manufacturer certificate signed securely by the manufacturer on a module produced in accordance with the approved process, where in addition to being the issuer, the Certification authority is also the manufacturer (Column 4, lines 30-35) and signs the certificate in accordance with the process. (Column 4, lines 54-61)
- Upon connection to the network of a terminal containing a module, verifying the signature to determine whether it is the manufacturer's signature, where anyone who has the public key of the CA, or manufacturer can verifying the signature. (Column 3, line 65- Column 4, line 9)

In reference to claim 20:

Puhl et. al discloses a method wherein the manufacturer certificate is signed using the manufacturer's private key such that on connection to the network a public key certificate is obtained with which to verify the signature, where the public key certificate is obtained (Column 12, lines 11-20) and where the manufacturer certificate is CA public key certificate and the private key is the private key of the CA. (Column 3, line 58 – Column 4, line 9)

In reference to claim 21:

Puhl et. al discloses a method wherein the verification of the signature is carried out by the issuer, where the issuers are Certification authorities, and Certification authorities may also verify each other's signatures in a process called Cross certification. (Column 10, lines 39-55)

In reference to claim 22:

Puhl et. al discloses a method wherein following successful verification of a signature, a further public key certificate is made available to support transactions with the terminal, the public key having been stored in the manufacturer certificate, where verifying the signature stems from verifying the certificate and enrollment onto the domain/network makes available the public key certificate to support transactions, where the public key is stored in the manufacturer's certificate. (Column 12, lines 18-20)

In reference to claim 23:

A module as claimed in claim 2, further including a certification authority certificate. (Column 5, lines 58 – 61)

Claims 24 and 25 are rejected for the same reasons as claim 4.

Claims 26-28 are rejected for the same reasons as claim 12.

Claims 29-31 are rejected for the same reasons as claim 6.

Claim 32 is rejected for the same reasons as claim 10.

Claims 33-36 are rejected for the same reasons as claim 12.

Claim 37 is rejected for the same reasons as claim 21.

Claims 38 and 39 are rejected for the same reasons as claim 22.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- US Patent 6,212,372
- US Patent 5,473,692
- PCT WO 01/43472A1
- Wireless Application Protocol Identity Module Specification, Part: Security Version 05, Nov 1999

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

January 6th 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100